ucd-snmp and net-snmp security update - (RHSA-2005-373 RHSA-2005-720)

Advisory Original Release Date: October 18, 2005
Last Revised: October 18, 2005
Number: ASA-2005-225
Risk Level: Low
Advisory Version: 1.0

Advisory Status: Interim

Overview:

SNMP (Simple Network Management Protocol) is a protocol used for network management.

A security vulnerability was discovered in net-snmp and in ucd-snmp. A denial of service bug was found in the way net-snmp and ucd-snmp use network stream protocols. It is possible for a remote attacker to send a net-snmp agent or a ucd-snmp agent a specially crafted packet which will crash the agent. The Avaya Modular Messaging Message Storage Server (MSS) ships with ucd-snmp installed, and is therefore vulnerable to this issue. No Avaya System Products ship with net-snmp installed and are therefore not vulnerable. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the names CAN-2005-1740 and CAN-2005-2177 to these issues.

More information about these vulnerabilities can be found in the security advisories issued by Red Hat:

- https://rhn.redhat.com/errata/RHSA-2005-373.html
- https://rhn.redhat.com/errata/RHSA-2005-720.html

System Products with net-snmp installed: None

System Products with ucd-snmp installed:

Product	Affected S/W Version	Comments and Actions
Avaya™ Modular Messaging – Message Storage Server (MSS)	All versions	Follow Recommended actions below. An update is being considered for a future release.

Recommended Actions:

For Avaya Modular Messaging Message Storage Servers, if snmp is not configured and being used on the MSS, it can safely be turned off. Avaya also recommends that customers restrict local and network access to the server. This restriction should be enforced through the use of physical security, firewalls, ACLs, VPNs, and other generally-accepted networking practices until such time as an update

becomes available and can be installed.

Avaya Software-Only Products

Avaya software-only products operate on general-purpose operating systems. Occasionally vulnerabilities may be discovered in the underlying operating system or applications that come with the operating system. These vulnerabilities often do not impact the software-only product directly but may threaten the integrity of the underlying platform.

In the case of this advisory Avaya software-only products are not affected by the vulnerability directly but the underlying Linux platform may be. Customers should determine on which Linux operating system the product was installed and then follow that vendors guidance:

Software-Only Products

Product	Affected S/W Version	Actions
Avaya™ CVLAN	All versions	Depending on the Operating System provided by customers, the affected package may be installed on the underlying Operating System supporting the CVLAN application. The CVLAN application does not require the software described in this advisory. Avaya recommends that customers follow recommended actions supplied by the Operating System vendor (e.g. Red Hat) or remove the affected package.
Avaya™ Integrated Management (AIM)	All versions	Depending on the Operating System provided by customers, the affected package may be installed on the underlying Operating System supporting the Integrated Management application. Avaya recommends that customers follow recommended actions supplied by the Operating System vendor (e.g. Red Hat).

Additional Information: Additional information may also be available via the Avaya support website (http://support.avaya.com) and through your Avaya account representative. Please contact your Avaya product support representative, or dial 1-800-242-2121, with any questions.

ELIMINATE SECURITY OR VIRUS THREATS TO CUSTOMERS' SYSTEMS. IN NO EVENT SHALL AVAYA BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE INFORMATION OR RECOMMENDED ACTIONS PROVIDED HEREIN, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF AVAYA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE INFORMATION PROVIDED HERE DOES NOT AFFECT THE SUPPORT AGREEMENTS IN PLACE FOR AVAYA PRODUCTS. SUPPORT FOR AVAYA PRODUCTS CONTINUES TO BE EXECUTED AS PER EXISTING AGREEMENTS WITH AVAYA.

Revision History:

V 1.0 - October 18, 2005 - Initial statement issued.

Send information regarding any discovered security problems with Avaya products to either the contact noted in the product's documentation or securityalerts@avaya.com.